1. A distributed computing system allowing secure external access to a secure network, the system comprising:

a target server within the secure network;

a border server within the secure network, the border server connectable to the target server by a first communications link;

a client outside the secure network, the client connectable to the border server by a second communications link, the client and the border server configured to support secure sockets layer communication over the second communications link;

a user authentication system located at least partially within the secure network, the secure network configured to allow direct access to the target server by a user only after the user is authenticated by the user authentication system; and

a uniform resource locator transformer which modifies non-secure uniform resource locators in data being sent from the target server to the client by replacing them with corresponding secure uniform resource locators to promote continued use of secure sockets layer communication.

2. The system of claim 1, wherein the uniform resource locator transformer is located on the border server.

3. The system of claim 1, wherein the uniform resource locator transformer is located on the target server and the system further comprises tunneling software for tunneling between the client and the target server through the border server.

4. The system of claim 1, wherein the secure network is configured to allow direct access to the target server from network addresses within the secure network while denying direct access to the target server from network addresses outside the secure network.

5. The system of claim 1, wherein the secure network includes a secured intranet.

6. The system of claim 1, wherein the client is a multi-user client.

7. The system of claim 6, wherein at least two user workstations are connected to the client.

8. The system of claim 1, wherein the user authentication system includes a Novell Directory Services database.

9. The system of claim 1, wherein the user authentication system includes a Microsoft Windows NT Domain directory.

10. The system of claim 1, wherein the user authentication system authenticates the user to all servers in the secure network after recognizing a single user name and a single corresponding user password.

11. The system of claim 1, further comprising a redirector for redirecting to the border server a request made by the client for direct access to the target server.

12. The system of claim 1, wherein the border server includes at least one cache.

13. The system of claim 12, wherein the border server cache includes data from the target server which contains non-secure uniform resource locators, and the uniform resource locator transformer introduces secure uniform resource locators on the fly without requiring that the transformed data also be cached on the border server.

14. The system of claim 12, wherein the border server cache includes a non-secure data cache for internal clients and a secure data cache for external clients, the non-secure data cache holding data that contains non-secure uniform resource locators, and the secure data cache holding data that does not contain non-secure uniform resource locators.

15. The system of claim 12, wherein the border server cache is free of data that contains non-secure uniform resource locators.

16. A method for providing access to a secure network, the method comprising the steps of:

receiving a request for access to a target server which is within the secure network, the access request having been made by a user outside the secure network;

forming a secure sockets layer connection between the user and a border server which is within the secure network;

using the secure sockets layer connection and a user authentication system of the secure network to authenticate the user to the secure network;

modifying data by replacing non-secure uniform resource locators in the data with corresponding secure uniform resource locators which promote continued use of secure sockets layer communication; and

transmitting the modified data to the user over a secure sockets layer connection.

17. The method of claim 16, wherein the modifying step is preceded by the step of transmitting the data to be modified from the target server to the border server in response to the access request, and the modifying step is performed at the border server.

18. The method of claim 17, further comprising the step of caching data on the border server.

19. The method of claim 16, wherein the modifying step is performed at the target server, and the transmitting step transmits the modified data to the user over a secure sockets layer connection which tunnels through the border server.

20. The method of claim 16, wherein the receiving step includes receiving the access request at the target server and the method further comprises the step of redirecting the request to the border server before the forming step.

21. The method of claim 16, wherein the forming step includes storing an IP address which indicates the current location of the user, and the step of transmitting the modified data to the user transmits the data only to that same IP address.

22. The method of claim 16, wherein the forming step forms a Netscape SSL connection.

23. The method of claim 16, wherein the using step includes obtaining from the user a user name and a user password.

24. The method of claim 16, wherein the step of modifying the data includes replacing the string "http" with the string "https" in at least one uniform resource locator.

25. A signal embodied in a computer system, the signal comprising a delimited non-secure uniform resource locator adjoined to a secure uniform resource locator, the non-secure uniform resource locator identifying a target server in a secure network, the secure uniform resource locator identifying a border server in the secure network.

26. The signal of claim 25, wherein the secure uniform resource locator identifies a specific port on the border server.

27. The signal of claim 25, wherein the non-secure uniform resource locator is delimited by quotes.

28. A computer storage medium having a configuration that represents data and instructions which will cause performance of method steps for providing access to a secure network, the method comprising the steps of:

receiving at a target server which is within the secure network a request for access to the target server, the access request having been made by a user outside the secure network;

redirecting the request to a border server which is within the secure network;

forming a secure connection between the user and the border server, the secure connection utilizing at least a transport layer protocol and lower level protocols, security in the connection being provided at least by encryption performed above the transport layer protocol;

using the secure connection and a user authentication system of the secure network to authenticate the user to the secure network;

modifying data by replacing non-secure uniform resource locators in the data with corresponding secure uniform resource locators which promote continued use of secure communication; and

transmitting the modified data to the user over a secure connection.

29. The configured storage medium of claim 28, wherein the forming step includes storing an IP address and a session identifier which collectively indicate the current location of the user, and the step of transmitting the modified data to the user transmits the data only to that same IP address and session.

30. The configured storage medium of claim 28, wherein the using step includes obtaining from the user a user name and password for network-wide authentication.

31. The configured storage medium of claim 28, wherein the modifying step is preceded by the step of transmitting the data to be modified from the target server to the border server in response to the access request, and the modifying step is performed at the border server.

32. The configured storage medium of claim 31, wherein the method further comprises the step of caching data on the border server.

33. The configured storage medium of claim 28, wherein the modifying step is performed at the target server, and the transmitting step transmits the modified data to the user over a secure sockets layer connection which tunnels through the border server.